The HIPAA Implementation Newsletter
Issue #28 – Friday - February 22, 2002
| Privacy | Contingency Planning | Project Planning | Security |
Web format with links at http://lpf.com/hipaa

___Privacy: Privacy Officer Survey___

HIPAA has made privacy a special concern for healthcare, but others are also feeling pressure and taking action. An October survey of privacy officers in consumer-services industries sponsored by Privacy & American Business and the Association of Corporate Privacy Officers and conducted by Opinion Research Corporation shows:

* 70% are now conducting a privacy-risk assessment of all personal information their company collects, how it is used and what kinds of privacy issues are involved; 22% plan to do this.
* 69% have a permanent Privacy Task Force of representatives from various business units and staff functions in their organizations; 15% plan to do this.
* 66% have a privacy policy covering all consumer information uses in their offline operations; 25% plan to do this.
* 62% have designated a privacy representative in all business units handling personal information to help oversee policy implementation and raise issues of concern; 18% plan to do this.
* 57% are operating a formal complaint and resolution program for consumers; 33% plan to do this.
* 56% are managing privacy training for company employees; 39% plan to do this.
* 37% are conducting a regular privacy audit of company operations that involve personal consumer information; 49% plan to do this.

CPOs Today:
* 78% have backgrounds in privacy-relevant functions, such as legal, public or government affairs, marketing, information technology, or management, with a third having previously had privacy responsibilities in those posts.
* 67% of privacy officials have worked in the business world for 11 years or more (20% for over 20 years); only 7% have been business workers less than three years.
* Reflecting their years of service and professional qualifications, 57% earn more than $100,000 yearly (46% earn between $100-200,000 and 11% over $200,000). Not surprisingly, persons designated by their organizations as "Chief Privacy Officer" are the highest paid.
* About half (48%) of these privacy officials have full time professional staff support (other than administrative). Forty-three percent of these have three or more staffers under their direction.
* When asked what percentage of the U.S. business community they think

will
have a designated privacy officer within the next three years, 40% believe more than half of U.S. firms will do this. That would produce something like 20,000 privacy officers across industries such as financial services, healthcare, telecommunications, retailing, and online firms. [All competing for limited resources.]
+More at: http://www.pandab.org/cposurveyrelease.html

___Privacy: Public Concern___

"A new Harris Interactive survey finds that most consumers are still worried about how companies use their personal data. The survey, conducted online Nov. 5-11, finds that
* 75% of consumers are concerned that companies they patronize will provide
confidential information to other companies without permission.
* 70% worry that transactions may not be secure, and
* 69% believe that hackers could steal their personal data. (Multiple answers were allowed.)
* 62% say that independent verification of policy adherence would mollify their concerns. Almost 85% say policy certification should be required."

COMMENTARY: Plan with the possibility that outside oversight of your privacy policies and their application could be required.
+From: InformationWeek Daily; Feb. 20
http://update.informationweek.com/cgi-bin4/flo?y=eF8z0BcnoF0V20WH0A5

___Contingency Planning: Based on Values___

"The concept of 'crisis' has been defined in a dozen ways, but from a management perspective, a crisis must be seen as a turning point in an organization's history. Crises are events that can cause … long-term or permanent reputational damage. [In the context of HIPAA, a breach of privacy
or security constitutes a crisis.]

"This planning model is based on values. Crises thrust an organization's values into the realm of public scrutiny. ... The crisis team must keep one thing in mind, above all, when anticipating and planning for crises: crises are fraught with risks, which present themselves immediately, and opportunities, which give small clues and only manifest themselves over time.

"In his excellent book, Defining Moments, Joseph L. Badaracco of Harvard Business School describes the reality of managers seeking to act on values as the need to "choose between right and right." These "…defining moments compel managers to reveal, test, and choose the ethics of their organization. Defining moments shape an organization because they cut

through all the finely crafted pronouncements about what the company aspires
to do and reveal instead what it actually does." This is especially true in crisis, as any manager who has been there can attest.

"It's Showtime when the crisis hits, and the audience will have little tolerance for actors who still have to read their lines."
+More at: http://www.bizforum.org/whitepapers/kamer.htm or http://kamergroup.com/resources.html (free registration required)

COMMENTARY: We like the addition of "organizational values" as part of the contingency planning process. It provides guidance for the planning process and a way of dealing with the contingencies that are not included in plans, like the events of September 11. The use of values in contingency planning also provides an opportunity to test and clarify the organization's statements about its values. Much of the contingency planning advice we have
seen deals with failure of systems and loss of facilities. That is important, but HIPAA also requires planning for situations where everything is available and working and there has been a breach of privacy and/or security. In those cases, the actions that are taken and the community perception of those actions will be driven by values. Brilliant execution that offends people will be seen as a failure.

___Contingency Planning: Fact Sheets___

"Here are Ten Fact Sheets every organization should prepare and keep on file for use by the media. There will be a need for these in the midst of a crisis – which is not the time to begin preparing them."
+More at: http://kamergroup.com/pdfs/Facts.pdf

___Project Planning: Legal___

"… legal planning … is as integral to success as technical planning. Negotiating a contract for a computer system, or for software, is - or should be - a systems planning process as much as it is an exercise in defining legal rights and duties. … In short, the aims of the contracting process are to:
* Explain the project to all parties, and develop an implementation plan;
* Furnish a process for discovering and accommodating the purchaser's new or changing requirements during the development and installation process;
* Supply a project management framework, including the means to adjust responsibilities and schedules as obstacles arise and as new needs are revealed;
* Preclude disputes, or specify a means for their quick resolution;
* Avoid litigation; and
* Establish a favorable litigation posture.
+More at:

http://www.dwt.com/practc/hc_ecom/publications/HIPAAChecklist.htm#b4

COMMENTARY: We provide litigation support regarding project management and
agree that the discipline provided by the attorneys could greatly reduce the risks of delays, cost over-runs and project failures. The two most common problems we see are inadequate definitions of roles regarding changes and change management, and the failure on the part of vendors to follow the project methodologies they describe before the sale.

___Security: Survey of Threats___

"Riptech's Internet Security Threat Report analyzes data produced by numerous brands of firewalls and intrusion detection systems used by hundreds of clients throughout the world... The rate of attack activity increased substantially over the past six months: Average attacks per company increased by 79% between July and December 2001.

"A substantial percentage of attacks appeared to be deliberately targeted at a specific organization, 39%, but 61% of attacks appeared to be opportunistic in nature (i.e., the attacker was broadly searching for any vulnerable system on the Internet).

"Impact of September 11th Terrorist Attacks: Excluding Nimda, there was no noticeable impact on attack activity during the week following September 11th. However, attack intensity rose precipitously within two weeks of the terrorist attacks. It is not clear whether there is a causal relationship, but the change in attack rates soon after September 11th is substantial."
+Request report from:
http://www.riptech.com/securityresources/form9.html

___Security: Wireless Vulnerabilities___

Wi-Fi networks used for portable online devices may be wide open to attacks according to a paper funded by the National Institute of Standards. The real problem is the fundamental way in which Wi-Fi works, according to the author
of the report, Professor Arbaugh.

"The next generation of security is TKIP and is backward-compatible with current Wi-FI products and upgradeable with software. TKIP is a rapid re-keying protocol that changes the encryption key about every 10,000 packets, according to Dennis Eaton, WECA chairman. TKIP will be available in the second quarter, said Eaton.

"But Arbaugh says TKIP does not eliminate the fundamental flaw in Wi-Fi security. 'If anybody breaks TKIP, they not only break the confidentiality but they also break the access control and authentication so one break

breaks everything.'

"Longer term, the IEEE Standards body intends to adopt AES [Advanced Encryption Standard], the same security protocol sponsored by the National Institute of Standards. "AES is state of the art encryption technology," said WECA chairman Eaton. But AES requires hardware acceleration using a co-processor to off-load the encryption and decryption or it would slow the throughput down to an unacceptable level, according to Eaton. It also requires new Wi-Fi cards in the client devices. AES will be available in the first quarter of 2003.
+More at:
http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml

___Security: Email___

Mail Policy Management: A 21st Century Business Imperative - META Group

"… to protect an increasingly mission-critical corporate communication asset, corporations will have to become far more aggressive in administration of email policy management. The issues that a comprehensive email policy management program must address include:

* Viruses can wreak havoc on corporate mail systems by compromising desktop
data, bringing down mail servers, and consuming precious mail manager resources. Organizations must be eternally vigilant against the constant threat of mail viruses.

* Organizations should filter outbound and inbound email content to protect trade secrets, reduce legal liabilities, reduce mailbox clutter and in some cases, comply with industry regulations/guidelines.

* Most organizations have the need to securely send email over the Internet to business partners, customers or their own employees. But most companies
do not yet have a corporate-wide solution for secure message delivery, thereby putting the company at risk.

* The lynchpin of mail policy management must be a codified policy that guides employee's use of the messaging system. Companies are advised to put
significant thought into devising these guidelines

Closely tied to these email hygiene issues is a rising volume of legal issues surrounding its use:
* Companies have been sued for violation of privacy for reading employees email;
* Employees have sued companies for receiving offensive messages;

* Companies have been sued by spam recipients after spammers had sent unsolicited commercial email through the corporate SMTP relay, thereby picking up the company's domain name;
* Companies have been held legally liable for libel in employee's email.

A sample user oriented email policy and procedure document is at the end of this report.
+Link to the Meta Group report from http://www.tumbleweed.com/en/

___Security: Firewalls 101___

A place to start if you need to buy a firewall or just need to be able to talk about firewalls with people who understand them.
+More at:
http://www.intranetjournal.com/articles/200202/se_02_13_02a.html

___We Have Been Recognized___

OnlineSecurity has elected to include compilations of articles from the HIPAA Implementation Newsletter on their "Intelligence Community Forum"

"One of the major challenges to the future evolution of the Internet and a wireless society is the development of effective privacy policies and the application of applied Internet security technology. It is the mission of OnlineSecurity to provide the services and products essential to the development of a secure worldwide information infrastructure, and for the online global protection of corporate and government assets."
http://www.onlinesecurity.com/
http://www.onlinesecurity.com/Community_Forum.php

___Update___
We have added:
A training category to the Background page with a link to privacy related training http://lpf.com/hipaa/background.html#training-background
A search engine and portal specifically for security and related issues to the Privacy and Security page
http://lpf.com/hipaa/privacy-security.html#security-tools
A portal to information about email policy including employer monitoring to the Privacy and Security page
http://lpf.com/hipaa/privacy-security.html#privacy-tools
Job descriptions for privacy and security officers to the Privacy and Security page
http://lpf.com/hipaa/privacy-security.html#privacy-job-descriptions-tools
Wireless Security Search Portal to the Privacy and Security page
http://lpf.com/hipaa/privacy-security.html#wireless-security-pands

___HIPAA Conferences___

HIPAA Summit West II March 13 - 15, 2002 San Francisco, CA
http://www.hipaasummit.com/HIPAAWest2/index.php3
With a faculty of more than 100 and 45 major content areas, the Summit will provide information on the status and construction of the HIPAA regulations through presentations by leading HIPAA regulators from the Department of Health and Human Services. It will provide specific and in depth analysis of state healthcare privacy and security laws. It will focus on practical case studies from the field, featuring presentations by leading privacy, security and compliance officers. Finally, it will address the complex financial, operational and technical issues of complying with the law and integrate new technologies to enhance the efficiency, quality and accessibility of healthcare services.

The Fourth Nationa lHIPAA Summit April 24-26, 2002 Washington, D.C.
http://www.hipaasummit.com/HIPAA4/index.php3
